PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/22, H04L 29/06

A1

(11) International Publication Number: **WO 98/32301**

(43) International Publication Date: 23 July 1998 (23.07.98)

(21) International Application Number: PCT/SE98/00022

(22) International Filing Date: 9 January 1998 (09.01.98)

(30) Priority Data:
08/784,152 17 January 1997 (17.01.97) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventor: NORDMAN, Mikael; Drotsvägen 16, S–191 33 Sollentuna (SE).

(74) Agent: BROMÉR, Britt; Ericsson Radio Systems AB, Common Patent Dept., S–164 80 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE ACCESS METHOD, AND ASSOCIATED APPARATUS, FOR ACCESSING A PRIVATE DATA COMMUNICATION NETWORK

(57) Abstract

A method (152), and associated apparatus (10), for accessing a private IP network (14) with a wireless host (32) by way of a wireless access network (52). Once authenticated and permitted access to the private IP network (14), the wireless host (32) becomes a virtual host of the private IP network (14). A wireless host identifier (WHI) is used to identify the wireless host (32). Permission to communicate by way of wireless access network (52) is confirmed by an authentication procedure (162). The WHI is thereafter provided to the private IP network (14). If the WHI is of a selected value, permission to access the private IP network (14) is granted. An IP address used to address data to the wireless host (32) is allocated by the private IP network (14) once access to the private IP network (14) is granted.

SECURE ACCESS METHOD, AND ASSOCIATED APPARATUS, FOR ACCESSING A PRIVATE DATA COMMUNICATION NETWORK

The present invention relates generally to communications between a wireless host and a network-located device. More particularly, the present invention relates to a method, and associated apparatus, for permitting the wireless host access to a private data communication network, such as a private IP network.

In an embodiment in which the private data communication network is formed of a private IP network, the private IP network is coupled to a wireless access network formed of the network infrastructure of a radio communication system, such as a cellular communication system. Once the wireless host is permitted access to the private IP network, an IP address is assigned to the wireless host by the private IP network. Information accessed at the private IP network is addressed to the wireless host using the IP address assigned by the private IP network.

A request by the wireless host to access the private IP network by the wireless host is transmitted first to the wireless access network. An authentication procedure is performed to confirm that the wireless host is permitted to communicate by way of the wireless access network. If the wireless host is authenticated, a wireless host identity (WHI), which identifies the wireless host is forwarded to the private IP network. The wireless host is permitted to access the private IP network if the WHI identifies a wireless host permitted to access the private IP network. The private IP network then allocates an IP address to the wireless host. The IP address is used to address data to the wireless host.

A simple and efficient manner by which to access a private IP, or other data communication, network is provided. A WHI is used to identify the wireless host in the wireless access network and at the private IP network. When the WHI is stored at the wireless access network, and does not have to be sent to the wireless access network infrastructure over an air interface. And, if the wireless host is permitted to access the private IP network, an IP address is assigned to the wireless host by the private IP network. The IP address can be dynamically allocated to the wireless host, and a separate IP address need not be permanently allocated to the wireless host.

to insure that the wireless host properly receives an acceptable level of access to the private network. That is to say, the wireless host should be treated as a virtual host, given the level of access to the private network as that given to a host physically coupled to such network.

Because the coupling of a wireless host to a network device of a private data communication network includes a radio link, the wireless host must be identified by an address so that data can be communicated thereto. In some existing communication systems in which a wireless host is able to communicate with a network device, the address of the wireless host is dynamically allocated. That is to say, e.g., in an embodiment in which the private data communication network is formed of a private IP network, rather than assigning a permanent IP address to the wireless host, a temporary IP address is assigned to the host when data is to be communicated to the wireless host. IPv6 dynamic IP address allocation is exemplary of an allocation method by which dynamically to allocate IP addresses to wireless hosts. In such method, to provide a fixed identity for the wireless host, a DNS (Domain Name System) name is allocated. A DNS name is a symbolic name provided for wireless hosts and other devices connected to an IP network.

One manner by which a wireless host can access a private IP network is to utilize a dial-out connection from the wireless host to the private IP network. Once a switched connection is formed, the wireless host is identified with a password.

Another manner by which a wireless host is sometimes able to access the private IP network is through the use of an authenticated tunnel. The wireless host is connected to the private IP network by way of the authenticated tunnel, and the wireless host is authenticated at the private IP network with an identity and a password. Such a tunneling method is sometimes referred to as "layer two tunneling." A PPTP system developed by MicroSoft Corporation, an L2F system developed by Sysco Systems, and an L2TP system developed by IETF are related to tunneling PPP.

The existing manners by which a wireless host accesses a private IP, or other data communication, network requires significant amounts of protocol overhead. As in any bandwidth-limited communication system, protocol overhead is width-consumptive.

infrastructure of the cellular communication system and the private IP network. It would, of course, be desirable for the wireless host instead to be able to access a wireless access network as close as possible to the location at which the wireless host is positioned and thereafter to utilize IP transmission between the wireless access network and the private IP network.

A manner by which better to permit access of a wireless host to access a private data communication network to communicate packet data therebetween would be advantageous.

It is in light of this background information related to access of a wireless host and to a private IP network that the significant improvements of the present invention have evolved.

SUMMARY OF THE INVENTION

The present invention advantageously provides a method, and associated apparatus, for permitting a wireless host access to a private data communication network, such as a private IP network. The present invention further advantageously provides a method, and associated apparatus, once access is granted to the private network, for dynamically allocating a temporary address to the wireless host. The dynamically-allocated address is used to address data which is to be communicated to the wireless host.

In one aspect of the present invention, the wireless host is coupled by way of an air interface to the network infrastructure of a PLMN (Public Land Mobile Network), such as a GSM network. The PLMN is, in turn, coupled to a private IP network. The network infrastructure forms thereby a wireless access network. When the wireless host requests access to the private IP network, communications are first authenticated at the wireless access network formed of the network infrastructure of the PLMN. An authentication procedure is performed to confirm that communications are permitted by way of the wireless access network. If the authentication procedure confirms that such communications are permitted, a wireless host identity (WHI), previously stored at the wireless access network and which identifies the wireless host, is forwarded to the private IP network. The private IP network permits access to the

communication station. The private data communication network is coupled to the network infrastructure of the radio communication system. A remote communication station identity is stored at the network infrastructure of the radio communication system. A registration request is generated by the remote communication station for requesting registration of the remote communication station to access the network infrastructure to permit the communication of data therethrough. The registration request is detected at the network infrastructure. The remote communication station is authenticated to confirm authorization of the remote communication station to communicate by way of the network infrastructure. A network-access request is forwarded to the private data communication network if the remote communication station is authenticated wherein the remote communication station is identified by the remote communication station identity. A determination is made, responsive to the network-access request, whether the remote communication station is permitted to access the private data communication network. And, the remote communication station is permitted to access the private data communication network if the remote communication station is determined to be permitted to access the private network. Subsequent to grant of permission to access the private data communication network, an address, such as a temporary address, can be assigned to the wireless host.

A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly summarized below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a functional block diagram of a communication system in which an embodiment of the present invention is operable.

Figure 2 illustrates a logical, functional block diagram illustrating the routing of data communicated between a wireless host and a private IP network.

Figure 3 illustrates a functional block diagram of a private IP network which includes an embodiment of the present invention for allocating an address by which to address data communicated to a wireless host.

a WHI (Wireless Host Identifier). Other subscriber data can additionally be stored at other storage locations of the SIM card 18.

The mobile terminal 16 is coupled to a wireless host 32, here by way of lines 34. The wireless 32, in one embodiment, forms a portable computer capable of receiving data communicated thereto by a network device of the private IP network 14. The wireless host 32 may alternately be coupled to the mobile terminal 16 by a contactless coupler, e.g., an infrared coupler. In one embodiment of the present invention, the wireless host 32 includes storage locations 36, 38, and 42 for storing data similar to that stored at the storage locations 24, 26, and 28. Namely, in such an embodiment, authentication information, the address of the private IP address 14, and the value of the WHI are stored at the storage locations 36-42, respectively. In the exemplary embodiment illustrated in the figure, such information is redundantly stored at the storage locations of both the SIM card 18 and the wireless host 32. In other embodiments, merely the authentication information is stored at one of the storage locations 24 or 36.

The network infrastructure of the communication system 10 forms a wireless access network which is coupled to the private IP network 14 by way of a backbone network 46. The wireless access network formed of the network infrastructure of the GSM system is here shown to include a BTS (Base Transceiver Station) 52. The BTS 52 is operable to generate downlink signals 54 and to receive uplink signals 56 upon an air interface formed of radio links between the remote communication station and the BTS 52.

In the embodiment in which portions of the communication system 10 are formed of a structure of a GSM communication system, such structure, as well as the air interface formed between the remote communication station 12 and the BTS 52 are defined by the specification standards of the GSM system.

Groups of BTSs, of which a single BTS 52 is shown in the figure, are coupled by way of lines 58 to a BSC (Base Station Controller) 62. The BSC 62 is operable, *inter alia*, to control operation of the BTSs coupled thereto. The BSC 62 is further coupled, here by way of lines 64, to a MSC/VLR (Mobile Switching Center/Visited Location Register) 66. The MSC/VLR 66 is operable in conventional manner to form

During operation, when an operator of the wireless host 32 desires to access the private IP network 14, appropriate commands are generated at the wireless host to initiate a request for access to the private IP network 14. Signals indicative of such request are provided to the mobile terminal 16, and the mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated. The BTS 52 forwards the request through the BSC 62 to the MSC/VLR 66.

The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out. While details of the authentication procedure carried out in a GSM communication system can be found in the specification standards of the GSM system, in general, the authentication procedure authenticates, i.e., confirms, that the mobile terminal 16 is permitted to communicate by way of the network infrastructure forming the wireless access network. Once the authentication procedure is successfully completed, i.e., the mobile terminal 16 is confirmed to be an authentic terminal which is permitted to communicate by way of the wireless access network formed of the network infrastructure, a value of the WHI associated with the wireless host is forwarded to the private IP network 14.

In one embodiment, when the WHI is stored at the HLR 76, the value stored thereat is provided by way of the line 86 to the SGSN 82, through the backbone 46 and to the private IP network 14. The WHI stored at the HLR is forwarded to the SGSN 82 if the authentication procedure confirms the authenticity of the mobile terminal 16. Thereby, the value of the WHI is authenticated by the authentication procedure performed by the wireless access network. Storage of the WHI at the HLR 76, or at another portion of the wireless access network, requires an agreement between an operator of the private IP network 14 and the operator of the wireless access network for the secure storage of the value of the WHI at the wireless access network. A separate IP address or DNS (Domain Name Service) name is provided only at the private IP network 14, and not elsewhere. Thereby, because the IP address and DNS name is provided at the private IP network, the wireless host 32, when permitted access to the private IP network, becomes a virtual host of the network 14. The user and host

invention, a wireless host, here the wireless host 32, is selectively permitted to access the private IP network, here again shown to form an HIPN, 14.

When the wireless host 32 is to gain access to the private IP network 14, the mobile terminal 16 generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system. The attachment procedure is performed pursuant to the SGSN 82 when using packet-switched circuit connections. And, the attach procedure is performed pursuant to the MSC/VLR 66 when circuit-switched circuit connections are used.

During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82. The other appropriate subscriber data includes the address of the private IP network 14. Addresses of additional private IP networks, such as the HIPN 96, 102, and 106 (shown in Figure 1) may also be downloaded to permit alternate, or second-choice access to an alternate IP network. The HIPN address identifying the private IP network 14, in one embodiment, is the address of the GGSN, such as the GGSN 92 of the private IP network 14.

Thereafter, the mobile terminal 16 generates a "PDP routing context activation request" to the SGSN 82 or an access to the MSC/VLR 66, as appropriate. The access to the MSC/VLR 66 is performed, for instance, by placing a call originated at the mobile terminal. Alternatively, standardization of additional protocol over the air interface to explicitly indicate that the MSC/VLR should be accessed can be made.

Pursuant to the activation request to the SGSN 82 or the access to the MSC/VLR 66, an indication of which HIPN is to be accessed is further provided to the SGSN or MSC/VLR, as appropriate. The mobile terminal 16 indicates, for instance, that the private IP network identified by the HIPN address stored at the HLR is the address of the private IP network which is to be accessed. Alternatively, the mobile terminal 16 can itself provide the address of the private IP network which is to be accessed. Or, a default address can be used to identify the private IP network which is to be accessed.

The WHR 124 is formed of a router having special support for selectively permitting a wireless host, such as the wireless host 32, to become a virtual host of the network. The network 14 includes other routers, here routers 126 and 128, which are connected to an Internet 132 and an intranet 134, respectively. The routers 124-128 are connected by way of a local area network (LAN) 138 to which a DHCP (Dynamic Host Configuration Profile) device 142 and a DNS (Domain Name Service) device 144 are also coupled. Other, optional application servers, of which the server 146 is representative, are also shown in the figure, also connected to the LAN 138. And, wireless hosts 148, directly coupled to the private IP network 14 are further pictured in the figure in connection with the LAN 138.

The DHCP 142 is operable to allocate addresses to wireless hosts, such as the wireless host 32. A WHI value is used as a wireless host address at the DHCP 142. The DNS 144 is operable to store names of the wireless hosts, such as the wireless host 32. The value of the WHI is used as a primary name at the DNS 144, and other secondary names can also be stored in conjunction with the WHI. Exemplary, DNS names include, for instance, WHI24450123456789@org.country; MSISDN467051234567@org.
country; and myhost@org.country.

The value of the WHI can be advantageously utilized because such value is a secure, wireless-network-provided identity which unambiguously identifies the wireless subscription used at the wireless host. By storing the value of the WHI as subscriber data at the HLR 76 (shown in Figure 1), the value of the WHI is stored with an appropriate level of security. As the wireless host accessing the GSM network is authenticated prior to receiving permission to use the WHI stored thereat, no separate log-in is needed to access the private IP network 14.

Transmission between the private IP network 14 and the wireless access router 124 must be secure. To ensure security of the transmission, the wireless host router 124 and the wireless access router forming a portion of the GSM, the wireless access network stores the address and authentication information about the respective routers between which communication is permitted. Such measures ensure that a WHI arriving at the wireless host router 124 is secure and correct. If necessary, transmission

block 162, to confirm authorization of the remote communication station to communicate by way of the network infrastructure.

Thereafter, an IP network-access request is forwarded to the private IP network, as indicated by the block 164. Then, as indicated by the block 166, a determination is made as to whether the remote communication station is permitted to access the private IP network.

And, the remote communication station is permitted to access the private IP network if the remote communication station is determined to be permitted to access the network.

During operation of an embodiment of the present invention permits a wireless host to become a virtual host of a private IP network. A wireless host identity (WHI) is used as a host identifier in the private IP network. The wireless host need only authenticate itself at the private IP network when no contract for safe storage exists between the operators of the wireless access network and the private IP network, regarding security of, e.g., identification information. An authentication procedure confirms the authenticity of the structure transmitting the access request. Bandwidth required over the air interface to generate the request to access the private IP network is advantageously also reduced when transferring IP packets over the air interface as only air-interface-specific protocols are used to transfer IP packets over the air interface.

The previous descriptions are of preferred examples for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is defined by the following claims.

method of accessing the private IP network by the remote communication station, said method comprising the steps of:

storing a remote communication station identity which identifies the remote communication station at a storage location;

generating a request by the remote communication station to access the network infrastructure to permit communication of data therethrough;

detecting at the network infrastructure the request generated during said step of generating;

authenticating the remote communication station to confirm authorization of the remote communication station to communicate by way of the network infrastructure;

forwarding an IP network-access request to the private IP network if the remote communication station is authenticated during said step of authenticating, the remote communication station identified by the remote communication station identity stored during said step of storing;

determining, responsive to the IP network-access request forwarded during said step of forwarding, whether the remote communication station is permitted to access the private IP network; and

permitting the remote communication station to access the private IP network if the remote communication station is determined, during said step of determining, to be permitted to access the private IP network.

3. The method of claim 2 wherein the storage location at which the remote communication station is stored during said step of storing is located at the network infrastructure of the radio communication system, the remote communication station identity stored together with authentication data associated with the remote communication station.

4. The method of claim 2 wherein the remote communication station comprises a wireless host coupled to a radio transceiver, the radio transceiver operable to communicate with the network infrastructure, and wherein said step of storing

11. The method of claim 2 wherein the radio communication system comprises a cellular communication system, wherein the data communicated between the remote communication station and the private IP network comprises packet-switched data, and wherein the request generated during said step of generating is provided to a router which by way of a circuit-switched circuit connection.

12. The method of claim 11 wherein the cellular communication system comprises a GSM communication system and wherein the router to which the request is provided comprises an MSC/VLR (Mobile Switching Center/Visited Location Register).

13. The method of claim 2 wherein said step of storing further comprises the step of storing a private IP network identity identifying the private IP network between which the data is communicated with the remote communication station.

14. The method of claim 13 wherein the IP network-access request forwarded during said step of forwarding is forwarded to the IP network identified by the IP network identity stored during said step of storing the private IP network identity.

15. The method of claim 2 wherein said step of generating further comprises generating a wireless-host-provided, IP network identity, the wireless-host-provided, IP network identity identifying the private IP network between which the data is to be communicated with the remote communication station.

16. The method of claim 15 wherein the IP network-access request forwarded during said step of forwarding is forwarded to the private IP network identified by the wireless-host-provided IP network identity generated during said step of generating.

17. The method of claim 2 wherein the remote communication station has associated therewith a default-IP network identity and wherein the IP network-access

communication network by the remote communication station, said apparatus comprising:

a storage element for storing a remote communication station identity identifying the remote communication station;

a detector coupled to the wireless access network infrastructure, said detector for detecting a request requesting access of the remote communication station to the wireless access network to permit communication of data therethrough;

an authenticator coupled to the wireless access network, said authenticator for confirming authorization of the remote communication station to communicate by way of the wireless access network;

a network access requestor coupled to said authenticator, said network access requestor operable responsive to authentication by said authenticator, said network access requestor for generating a request to request access to the private data communication network by the remote communication station, the remote communication station identified in the request by the remote communication station identifier stored in said storage element; and

a determiner positioned at the private IP network, said determiner operable responsive to the request requested by said network access requestor to determine whether to permit access by the remote communication station to the private data communication network.

23. The apparatus of claim 22 further comprising an address allocator positioned at the private IP network, said address allocator for allocating an address to the remote communication station, the address allocated by said address allocator used to address data communicated to the remote communication station by the private IP network.

24. The apparatus of claim 23 wherein said address allocator comprises a dynamic allocator for dynamically allocating a temporary IP address, the temporary IP address used to address the data communicated to the remote communication station for a selected period.

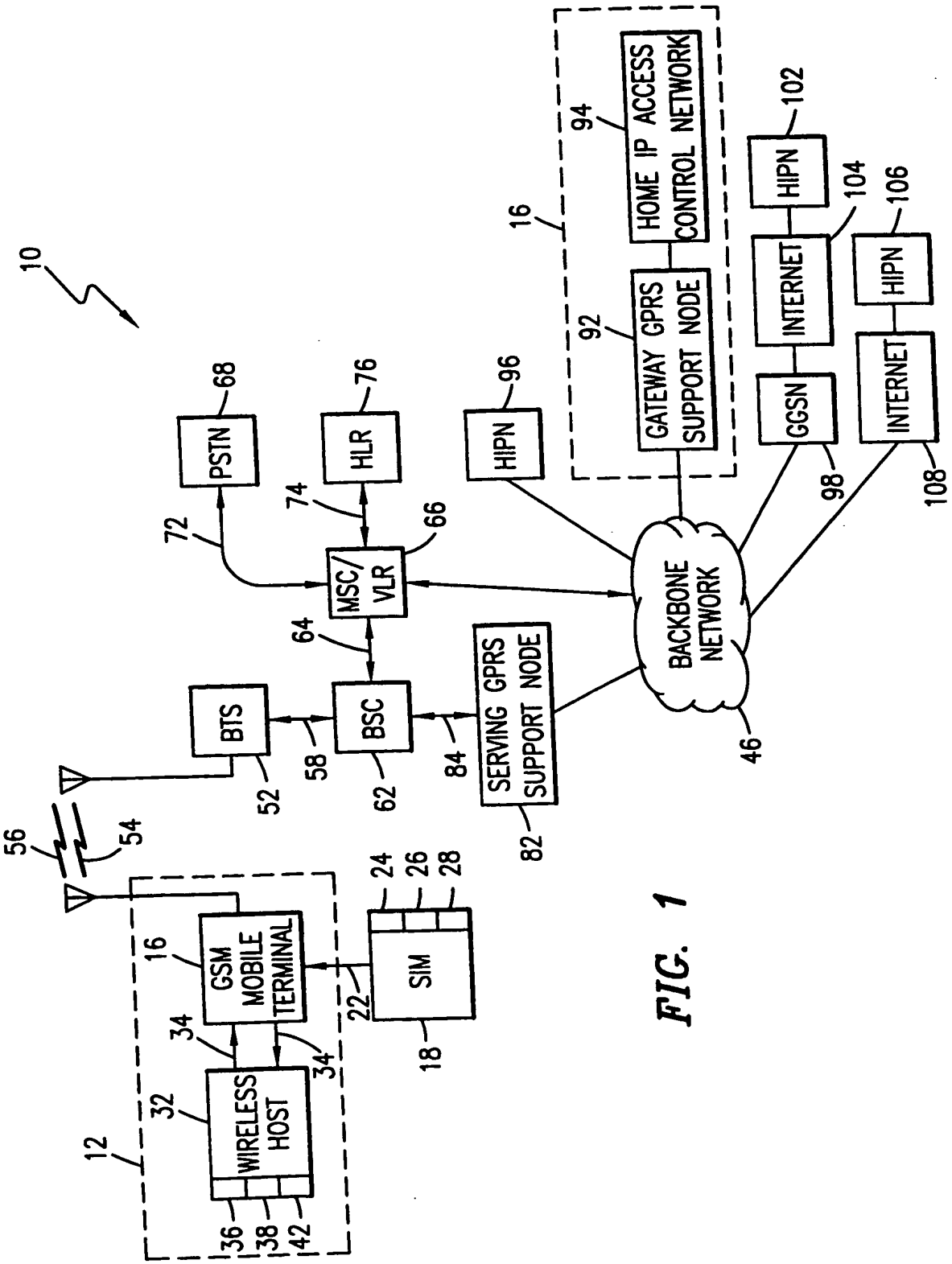
10
12
16
GSM MOBILE TERMINAL
WIRELESS HOST
SIM
18
22
24
26
28
32
34
36
38
42
46
52
54
56
58
62
64
66
68
72
74
76
82
84
92
94
96
98
102
104
106
108
BTS
BSC
MSC/ VLR
PSTN
HLR
HIPN
SERVING GPRS SUPPORT NODE
BACKBONE NETWORK
GATEWAY GPRS SUPPORT NODE
HOME IP ACCESS CONTROL NETWORK
GGSN
INTERNET
HIPN
INTERNET
HIPN

FIG. 1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 98/00022

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 483 547 A (IBM) 6 May 1992	1,2,4, 13, 17-19, 22-25
Y	see abstract	8,9,11
A	see column 4, line 19 - column 5, line 28; figures 2-4	5-7,10, 12, 14-16, 20,21
	see column 6, line 49 - column 7, line 19	
	see claims 1,2,9	

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

2

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 1998	17/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cichra, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/SE 98/00022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0483547 A	06-05-92	US 5159592 A	27-10-92
		DE 69119353 D	13-06-96
		DE 69119353 T	07-11-96
		JP 2516291 B	24-07-96
		JP 4227149 A	17-08-92